Digital Signature pada Citra Digital dengan Algoritma *Least Significant Bit* dan *Chaocipher*

Sandy Juniart Siwabessy [1], **Magdalena A. Ineke Pakereng** [2]
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesia
E-mail: 672010264@student.uksw.edu[1], ineke.pakereng@staff.uksw.edu[2]

Abstract

Documents in the form of digital image has the possibility to be manipulated unlawfully. The information contained within can be faked, so that the recipient of the document can be wrong in interpreting the intention of the information therein. This could result in losses for both the sender and recipient document, the decision made, based on the information that has been falsified. A solution is needed to secure the information stored on it. Information from the sender must be the same when it reached the receiver. In this study generated digital signature applications implemented in a way that is calculating the value of bytes of data into a form MD5 hash algorithm. Results hash is then encrypted with an algorithm Chaocipher. Cipher hash then inserted at Least Significant Bit of digital images. Digital signature is inserted can be used to detect whether the digital image has been changed or not. The test results showed that the change can be detected, even if the change only by 2x2 pixels.

Keywords*: *Digital Signature, Least Significant Bit Embedding, Chaocipher

Abstrak

Dokumen berbentuk citra digital memiliki kemungkinan untuk dimanipulasi secara tidak sah. Informasi yang terdapat di dalamnya dapat dipalsukan sehingga pihak penerima dokumen dapat salah dalam menginterpretasikan maksud informasi di dalamnya. Hal ini dapat mengakibatkan kerugian baik bagi pengirim dokumen maupun penerima dokumen, karena keputusan yang dibuat, berdasarkan pada informasi yang telah dipalsukan. Sebuah solusi diperlukan untuk mengamankan informasi yang tersimpan di dalamnya. Informasi dari pengirim harus sama ketika sampai di penerima. Pada penelitian ini dihasilkan aplikasi *digital signature* diimplementasikan dengan cara yaitu menghitung nilai *byte* data menjadi bentuk *hash* dengan algoritma MD5. Hasil *hash* kemudian dienkripsi dengan algoritma *Chaocipher*. *Cipher hash* kemudian disisipkan pada bagian *Least Significant Bit* citra digital. *Digital signature* yang disisipkan tersebut dapat berfungsi untuk mendeteksi apakah citra digital telah mengalami perubahan atau tidak. Hasil pengujian menunjukkan bahwa perubahan dapat terdeteksi, sekalipun perubahan hanya sebesar 2x2 piksel.

Kata Kunci: Tanda Tangan Digital, Penyisipan *Least Significant Bit*, *Chaocipher*

---

[1] Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga
[2] Staf Pengajar Fakultas Teknologi Informasi Universitas Kristen Satya Wacana Salatiga